International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-006 PAGE NO: 029-033

Attacks Detected by Discovery and Distance Vector Protocols in Ad-hoc Networks

S.Vijayakumar [#1], P.Kaleeswari [*2]

[#1] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
vijayakumar003@gmail.com

[*2] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
kaleeswarip27@gmail.com

Abstract— **The research aims for detection and provide the counter measure for attacks such as misrouting, identity delegation, colluding collision, colluding injected attack and power control in the wireless adhoc networks. The above mentioned attacks easily encountered in wireless adhoc networks. Due to these attacks many packets are dropped in the intermediate path before reaching the destination. The research introduce the protocol called SNDP (Secure Neighbor Discovery Protocol) that can detect these attacks and isolate packet dropping attack efficiently and use reactive routing protocol such as AODV(Ad-Hoc On-demand Distance Vector) technique to provide the counter measure for preventing the packet loss against misrouting.**

Keywords: Misrouting, Identity Delegation, Colluding Collision, Power Control, Colluding Injected Attack, SNDP Protocol, AODV protocol and Guard node**.**

I. INTRODUCTION

The popularity of wireless ad hoc network has been growing very rapidly because they are very easy to implement without using base stations. The wireless ad hoc networks are complex distributed systems that consist of wireless mobile or static nodes that can freely and dynamically self-organize. Moreover it provides advantage such as easy portable, which is increasingly used in rescue mission, especially for accessing rough terrains. But in wireless ad hoc network, due to the unconstrained network topology changes, route changes and network partitions occur frequently [1].

Wireless ad hoc networks are most important platform in military warfare and control of civilian critical infrastructure. In these networks the malicious behavior node may enter into the network and perform [5].

We introduce the secure neighbor discovery protocol (SNDP) that is used to detect the malicious node enter into the

System [9]. This protocol has 2 principles to detect and control the attacker's behavior. First, during communication between source and destination, the guard node is established and distributes the key to neighbor nod. Second, check whether the neighbor node is legitimate node or not. Based on this technique we can detect the 5 attacks. Our contributions are as follows:

- We will explain the five different types of attacks, misbehavior like packet dropping and how these problems. Enter into the wireless ad hoc networks.
- We introduce the SNDP protocol to protect against these attacks with added the resource consumption and node responsibility.
- We use AODV protocol to protect against the misrouting attack.
- We show the security advantage of SNDP and AODV protocols in wireless ad hoc networks through

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-006 PAGE NO: 029-033

analysis and simulations.

II. ATTACKS IN WIRELESS NETWORK

In this section describes the five types of attacks such as misrouting, identity delegation, colluding injected attack, colluding collision and power control [1] [4].

1. .Misrouting:

In this type of attack, the node in the network relays the packet to an incorrect next-hop neighbor [2]. Due to this, the misrouted packet cannot reach its original destination. So the destination does not receive the entered data packets.

2. Integrity delegation:

In this type of attack, the attacker may act as any of the intermediate node or destination node [2]. The legitimate destination or intermediate node does not receive data packets because the attacker's malicious node can access the particular packet.

3. Colluding injected attack:

In this type of attack, the adversary will inject malicious nodes into the network, making sure they aren't noticed as malicious nodes. These nodes blend into the network, acting as legitimate nodes and plot against the arbitrary node. They prevent packets from reaching that node and then move on to attack the next node. This way the entire network gets affected [7].

4. Colluding collision:

In this type of attack [1] [2], the attacker uses the colluding node to transmit data at the same time when the original data transmit. Therefore collision may occur, which prevent the correct data from being received by the node, while the sending node appears to be performed its functionality correctly.

5. Power control:

In this type of attack, the attacker to reduce the power level from legitimate nodes. In this mode, malicious node controls the transmission power to relay the packet from the intermediate node. Due to this the packet never reaches the next hop [1] [2].

III. SNDP PROTOCOL

This secure neighbor discovery protocol provides the authorized path between the source and destination to make the communication by using the guard node. The guard node will monitor the entire wireless network and distribute the key only for the authorized node. In the wireless network every node has to check with the "HELLO PACKETS" and neighbor discovery & neighbor verification perform in the overall network with the key values [9].

Guard Node:

Guard node chosen by a user (sender or receiver) are not an attacker-controlled. User chooses the guard node depending on their need of flexibility. This guard node is better to increase the sender's and receiver's performance. Users who have good guard nodes, makes the situation that is much better when a sender or receiver picks a few nodes as its "guards". There is a small chance that the network circuit will be compromised. To help improve this situation the guard feature was implemented.

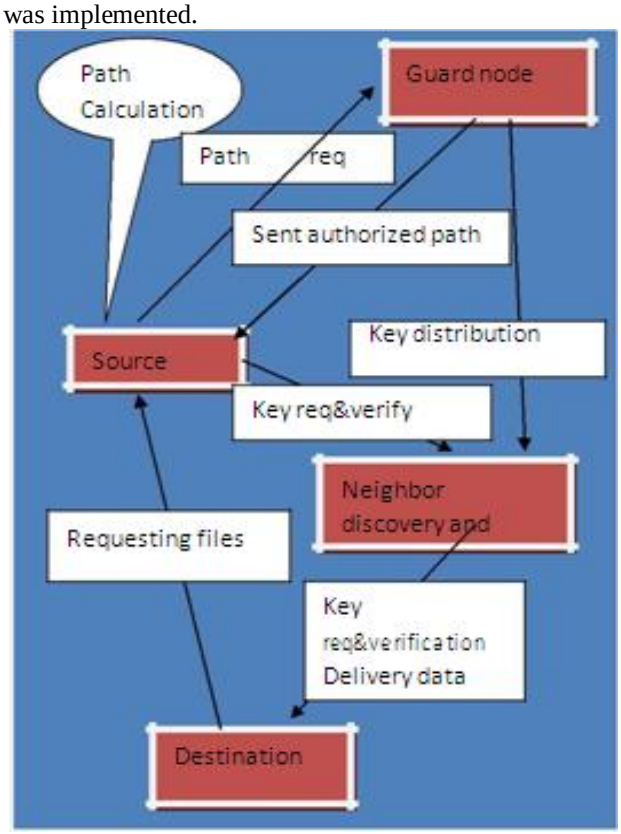


Figure 1: SNDP Protocol function.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-006 PAGE NO: 029-033

The SNDP Protocol work as follows:

1. First step is to construct the wireless sensor network

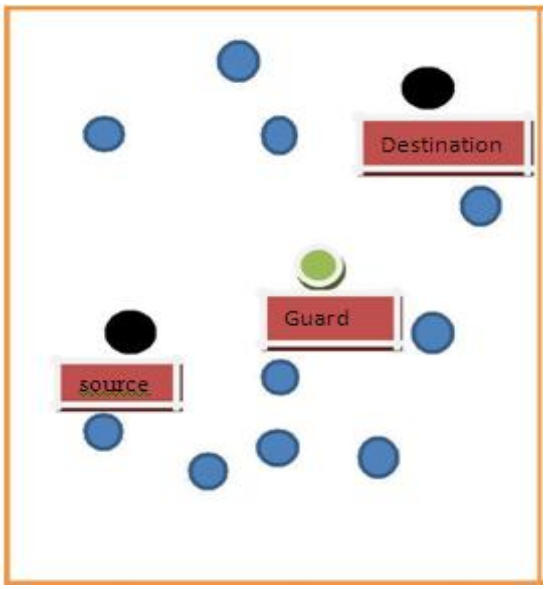


Figure 2: Wireless ad-hoc network

For example, the above wireless network is constructed with several nodes.

2. After constructing network, next step is to select the guard node for forwarding data packets.

   In the above example wireless network, one node act as a guard node ant it monitor the whole network.
3. Then next step is the destination node request to source node.
4. After requesting, source node sends the authorized path from guard node.
5. The guard node already knows the information about the both legitimate node and malicious nodes behavior.
6. The guard node next to find out the authorized path and distribute the key from authorized path.
7. Then source node sends the “hello packet” to its neighbor node before sending the data packet.
8. The neighbor node reply in 2 ways”

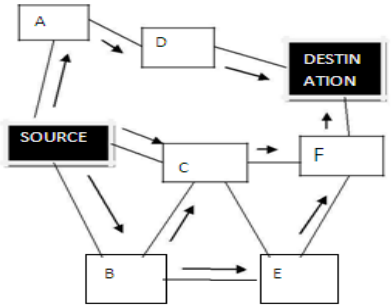
   Hello packet with key.
   Hello packet without key.
9. The node which sends the “hello packet with key” is moved to active state, the remaining nodes are moved to sleep state.
10. Continue this process up to the specified destination reached.
11. At last the data packets are delivered to the correct destination without loss [9].

IV. AODV PROTOCOL

AODV protocol is introduced to overcome the misrouting attack. In AODV protocol, each node maintains a routing table. Each entry records the next hop to reach destination and its hop count (the distance from the current node to the destination node). AODV protocol is based on DSDV and DSR [3] [8]. AODV finds a route through network, like DSR.

But unlike DSR, it doesn’t store the nodes it has passed but only counts the number of hops. AODV uses a sequence number generated by destination to indicate the fresh routes. The intermediate node are to check for fresh routes based on the hop count and sequence number and forwards the packets that they receive from their neighbors to the specified destinations.

AODV use the hello packets for route maintenance. If a node doesn’t receive a hello packet within a certain time, or it receives a misrouting signal, it sends a route error packet. Main difference between this protocol and DSR protocol is that, in DSR each packet carries full routing information, whereas in AODV the packets carry the destination address. So the AODV consumes less memory than DSR [3] [8]. The second difference is that the route reply packets in DSR carry the address of each and every node along the route, whereas the AODV the route reply only carry the destination address and sequence number.



Figure(3a).Sending procedure of a request packet

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-006 PAGE NO: 029-033

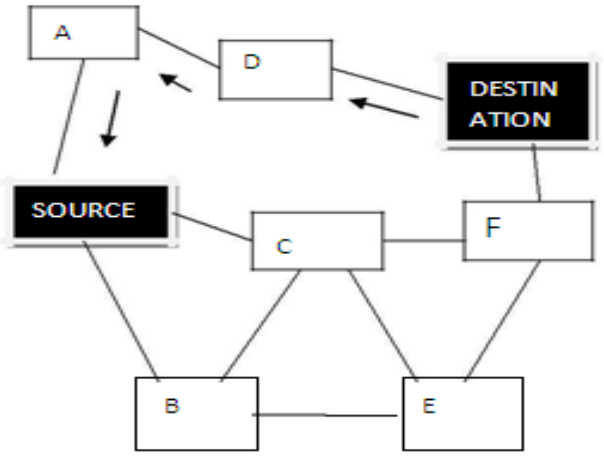


Figure (3b).Replying message for reply packet

V. ANALYSIS

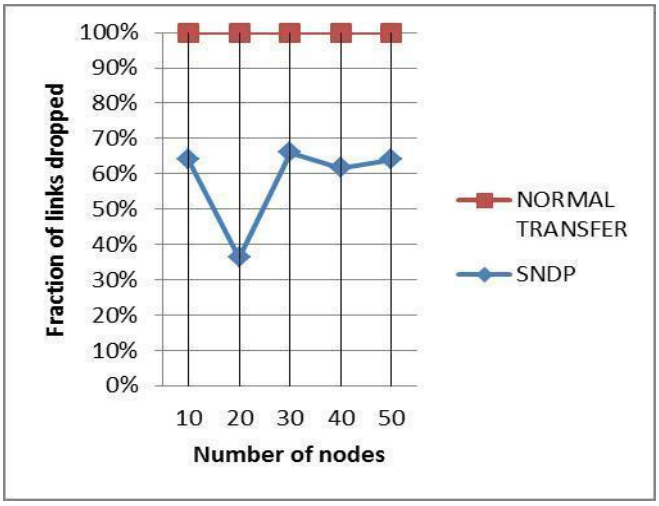


Figure 4:

Figure 4 explain the fraction of link dropped comparison between the normal transfer and SNDP protocol [9]. In the normal process the doped links are high compare to SNDP protocol. The normal transfer wireless network unnecessary to loss the packets because the redundant dropped links are appeared. To provide remedy for this problem, SNDP protocol is used. It reduces the unnecessary packet loss.

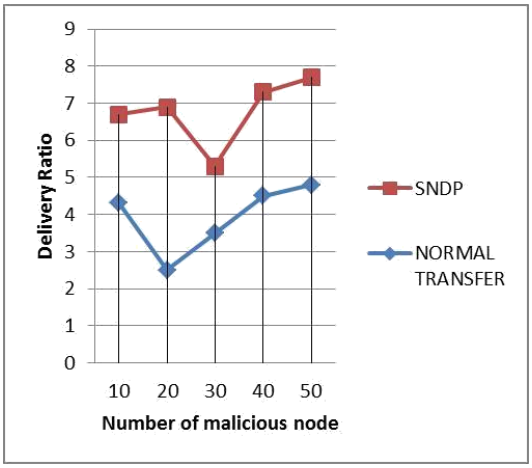


Figure 5:

The figure 5 explains the comparison ratio for delivery between the malicious node normal nodes. If normal transfer use some other protocol for wireless network, that time the malicious node increase the delivery ratio from their network. To overcome this issue uses the SNDV Protocol and its framework to reduce the unnecessary loss to data packets from their network [9].

Packet loss rate (%)	DSR		AODV	
	Static	Mobile	Static	Mobile
Tahoe	0.15	0.88	0.00	0.33
Reno	0.15	0.86	0.00	0.33
New Reno	0.15	0.44	0.00	0.33
Vegas	0.00	0.14	0.00	0.07
Westwood	0.13	0.12	0.04	0.51

Table 1. The percentage of packet loss rate in grid topology. It describes the AODV performance over DSR [3] [5] in grid topology.

VI.CONCLUSION

We have presented two protocols such as AODV and SNDP to detect the attacks in wireless ad-hoc network thereby, eliminate the packet loss. The malicious behavior

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-006 PAGE NO: 029-033

cannot be detected easily by using any other protocols. In this detection method expand into neighbors that are capable of monitoring in a neighborhood. So this approach is more suitable than other protocols. The output performance of SNDP is compared with the normal transfer process through analysis.. The detection of the attack using SNDP gives better performance in terms of reducing the packet loss [9].

In future, we can plan for developing detection techniques for multi-channel multi-media wireless networks.

This detection activity will be more complicated because multiple channels are presented.

VII. REFERENCES

[1] Issa Khalil and Saurabh Bagchi," Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure" IEEE transactions on mobile computing.

[2] May Zin Oo and Mazliza Othman "The Effect of Packet Losses and Delay on TCP Traffic over Wireless Ad Hoc Networks".

[3] DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, David B. Johnson David A.Maltz Josh Broch.

[4] Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy

[5] Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc. ACM Int'l Conf. Security and Privacy in Comm. Networks (Secure Comm '08).

[6] D. Johnson, D. Maltz, and J. Broch,"The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Counter measures in Mobile Ad hoc Networks," Wireless/Mobile Network Security pg 1-38.

[8] C. Perkins, Ad hoc Networks, Addison-Wesley, 2001. "Mcia-Mitigating Colluding Injected Attacks in Mobile Ad Hoc Networks"

[9] Y. C. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," ACM Workshop on Wireless Security (WiSe'03), pp. 30-40, 2003.

[10] S. Hariharan, N. Shroff, and S. Bagchi, "Secure Neighbor Discovery in Wireless Sensor Networks," Purdue Technical Report, TR ECE 07-19, 2007.

Published by SK Research Group of Companies (SKRGC).